Conference Matrices and Unimodular Lattices

Robin Chapman
School of Mathematical Sciences
University of Exeter
Exeter, EX4 4QE, UK
rjc@maths.ex.ac.uk

19 July 2000

1 Introduction

We use conference matrices to define an action of the complex numbers on the real Euclidean vector space $\mathbf{R}^n$. In certain cases, the lattice D_n^+ becomes a module over a ring of quadratic integers. We can then obtain new unimodular lattices, essentially by multiplying the lattice D_n^+ by a non-principal ideal in this ring. We show that lattices constructed via quadratic residue codes, including the Leech lattice, can be constructed in this way.

Recall that a *lattice* Λ is a discrete subgroup of a finite dimensional real vector space V. We suppose that V has a given Euclidean inner product $(\mathbf{u},\mathbf{v}) \mapsto \mathbf{u}\cdot\mathbf{v}$ and the rank of Λ equals the dimension of V. In this case Λ has a bounded fundamental region in V. We call the volume of such a fundamental region (measured with respect to the Euclidean structure on V) the *volume* of the lattice Λ.

The lattice Λ is *integral* if $\mathbf{u}\cdot\mathbf{v} \in \mathbf{Z}$ for all $\mathbf{u}$, $\mathbf{v} \in \Lambda$. It is *even* if $|\mathbf{u}|^2 = \mathbf{u}\cdot\mathbf{u} \in 2\mathbf{Z}$ for all $\mathbf{u} \in \Lambda$. Even lattices are necessarily integral. The lattice Λ is *unimodular* if Λ is integral and has volume 1. It is well known [9, Chapter VIII, Theorem 8] that if Λ is an even unimodular then the rank of Λ is divisible by 8.

For convenience we call the square of the length of a vector its *norm*. The *minimum norm* of a lattice is the smallest non-zero norm of its vectors.

2 Conference matrices

Let l be a positive integer. A *conference matrix* of order n [7, Chapter 18] is an n-by-n matrix W satisfying

(a) the diagonal entries of W vanish, while its off-diagonal entries lie in $\{-1, 1\}$,

(b) $WW^\top = (n-1)I$, where I denotes the n-by-n identity matrix.

Let $\mathcal{W}_n$ denote the set of skew-symmetric conference matrices of order n.

Let $W \in \mathcal{W}_n$. Then $H = I + W$ satisfies $HH^t = (I+W)(I-W) = I - W^2 = I + WW^\top = nI$. As all the entries of H lie in $\{-1, 1\}$ then H is a Hadamard matrix. Consequently [7, Theorem 18.1] $n = 1$, 2 or is a multiple of 4.

Suppose that n is a multiple of 4 and let $l = n - 1$. Fix $W \in \mathcal{W}_n$ and let $V = \mathbf{R}^n$ denote the n-dimensional real vector space under the standard Euclidean dot product. Then, since $W^2 = -lI$, V becomes also a complex vector space when we define

$$(r + s\sqrt{-l})\mathbf{v} = \mathbf{v}(r + sW)$$

for r, $s \in \mathbf{R}$. Let $|\mathbf{v}| = \sqrt{\mathbf{v} \cdot \mathbf{v}}$ denote the Euclidean length of a vector $\mathbf{v} \in \mathbf{R}^n$. This action of $\mathbf{C}$ on $\mathbf{R}^n$ transforms lengths in the obvious way. Let z^* denote the complex conjugate of the complex number z.

Lemma 2.1 *(a) If z_1, $z_2 \in \mathbf{C}$ and $\mathbf{v}_1$, $\mathbf{v}_2 \in \mathbf{R}^n$ then $(z_1\mathbf{v}_1) \cdot (z_2\mathbf{v}_2) = (z_1 z_2^* \mathbf{v}_1) \cdot \mathbf{v}_2$*

(b) If $z \in \mathbf{C}$ and $\mathbf{v} \in \mathbf{R}^n$ then $|z\mathbf{v}| = |z||\mathbf{v}|$.

Proof Let $z_j = r_j + s_j\sqrt{-l}$ with r_j, $s_j \in \mathbf{R}$. Then

$$\begin{aligned}
(z_1\mathbf{v}_1) \cdot (z_2\mathbf{v}_2) &= (z_1\mathbf{v}_1)(z_2\mathbf{v}_2)^\top \\
&= \mathbf{v}_1(r_1 I + s_1 W)(r_2 I + s_2 W)^\top \mathbf{v}_2^\top \\
&= \mathbf{v}(r_1 I + s_1 W)(r_2 I - s_2 W)\mathbf{v}^\top \\
&= \mathbf{v}((r_1 r_2 + l s_1 s_2)I + (s_1 r_2 - r_1 s_2)W)\mathbf{v}^\top \\
&= (z_1 z_2^* \mathbf{v}_1) \cdot \mathbf{v}_2
\end{aligned}$$

as claimed.

Consequently

$$|z\mathbf{v}|^2 = (z\mathbf{v}) \cdot (z\mathbf{v}) = (zz^*\mathbf{v}) \cdot \mathbf{v} = |z|^2 \mathbf{v} \cdot \mathbf{v} = |z|^2 |\mathbf{v}|^2.$$

□

Thus for fixed nonzero z, the map $\mathbf{v} \mapsto z\mathbf{v}$ is a similarity of $\mathbf{R}^n$ with scale factor $|z|$.

3 Quadratic fields

We retain the previous notation. Suppose in addition that $l = n - 1$ is squarefree. Let K denote the quadratic field $\mathbf{Q}(\sqrt{-l})$. Since l is square-free, the ring of integers of K is

$$\mathcal{O} = \mathbf{Z}\left[\frac{1+\sqrt{-l}}{2}\right] = \left\{\frac{a+b\sqrt{-l}}{2} : a, b \in \mathbf{Z}, a \equiv b \pmod 2\right\}.$$

In particular $\mathcal{O}$ is a Dedekind domain. We shall show that some of the familiar lattices in $\mathbf{R}^{l+1}$ are modules for the ring $\mathcal{O}$.

Let

$$L_0 = \{(a_1, \ldots, a_n) \in \mathbf{Z}^n : a_1 + \cdots + a_n \equiv 0 \pmod 2\}$$

be the D_n root lattice.

Lemma 3.1 *The lattice L_0 is an $\mathcal{O}$-module.*

Proof It suffices to show that $\frac{1}{2}(1+\sqrt{-l})\mathbf{v} = \frac{1}{2}\mathbf{v}(I+W) \in L_0$ whenever $\mathbf{v} \in L_0$. Indeed it suffices to show this whenever $\mathbf{v}$ lies in a generating set for L_0. Now L_0 is generated by the vectors $2\mathbf{e}_j$ and $\mathbf{e}_j + \mathbf{e}_k$ (for $j \neq k$) where $\mathbf{e}_j$ denotes the j-th unit vector. Firstly $\mathbf{e}_j(I+W)$ is a row of the Hadamard matrix $I+W$. As it contains n instances of ± 1 and n is even, it lies in L_0. Next $\frac{1}{2}(\mathbf{e}_j+\mathbf{e}_k)(I+W)$ is the sum of two rows of the Hadamard matrix $I+W$. Two rows of an n-by-n Hadamard matrix agree in exactly $n/2$ places. Hence $\frac{1}{2}(\mathbf{e}_j+\mathbf{e}_k)(I+W)$ has $n/2$ zeros and $n/2$ instances of ± 1. As $n/2$ is even then $\frac{1}{2}(\mathbf{e}_j+\mathbf{e}_k)(I+W) \in L_0$. This completes the proof. $\square$

Now consider the set

$$\mathcal{S} = \{(a_1, \ldots, a_n) : a_j \in \{-1/2, 1/2\}\}.$$

The difference of two vectors in $\mathcal{S}$ lies in L_0 if and only if those vectors agree in an even number of places. Thus there are exactly two cosets $\mathbf{v} + L_0$ as $\mathbf{v}$ runs through $\mathcal{S}$.

For each j, $\frac{1}{2}\mathbf{e}_j(I+W) \in \mathcal{S}$, and for each j and k, $\frac{1}{2}(\mathbf{e}_j - \mathbf{e}_k)(I+W) \in L_0$ by Lemma 3.1. Thus the cosets $\frac{1}{2}\mathbf{e}_j(I+W) + L_0$ are identical. Let

$$\mathcal{S}_+ = \{\mathbf{v} \in \mathcal{S} : \mathbf{v} - \tfrac{1}{2}\mathbf{e}_1(I+W) \in L_0\}$$

and

$$\mathcal{S}_- = \mathcal{S} \setminus \mathcal{S}_+.$$

As $\frac{1}{2}\mathbf{e}_j(I+W) - \frac{1}{2}\mathbf{e}_j(-I+W) = \mathbf{e}_j \notin L_0$ then $\frac{1}{2}\mathbf{e}_j(-I+W) \in \mathcal{S}_-$ for each j.

If $\mathbf{v} \in \mathcal{S}$ then $2\mathbf{v}$ has n entries ± 1 and so $2\mathbf{v} \in L_0$. It follows that $L_0 \cup (\mathbf{v} + L_0)$ is a lattice, which depends only on whether $\mathbf{v} \in \mathcal{S}_+$ or $\mathbf{v} \in \mathcal{S}_-$. We write L_+ for $L_0 \cup (\mathbf{v} + L_0)$ when $\mathbf{v} \in \mathcal{S}_+$ and L_- for $L_0 \cup (\mathbf{v} + L_0)$ when $\mathbf{v} \in \mathcal{S}_-$. Both L_+ and L_- are isometric to the lattice usually denoted by D_n^+ [5, Chapter 4, §7.3]. The lattice D_n^+ is unimodular for each n divisible by 4, and it is even unimodular whenever n is divisible by 8.

Lemma 3.2 *If n is divisible by 8 then the lattices L_+ and L_- are $\mathcal{O}$-modules.*

Proof Let $L = L_+$ or L_-. Then $L = L_0 + (\mathbf{v} + L_0)$ for some $\mathbf{v} \in \mathcal{S}$ and by Lemma 3.1 it suffices to show that $\frac{1}{2}(1 + \sqrt{-l})\mathbf{v} = \frac{1}{2}\mathbf{v}(I + W) \in L$. Note that $\frac{1}{4}(l + 1)$ is an even integer by the hypothesis.

We may assume that $\mathbf{v} = \frac{1}{2}\mathbf{e}_1(\pm I + W)$. If $\mathbf{v} = \frac{1}{2}\mathbf{e}_1(I + W)$ then

$$\frac{1}{2}\mathbf{v}(I + W) = \frac{1}{4}\mathbf{e}_1(I + W)^2 = \frac{1}{4}\mathbf{e}_1((1 - l)I + 2W) = \frac{1}{2}\mathbf{e}_1(I + W) - \frac{l + 1}{4}\mathbf{e}_1$$

which lies in L as $\frac{1}{2}\mathbf{e}_1(I + W) \in L$.

If $\mathbf{v} = \frac{1}{2}\mathbf{e}_1(-I + W)$ then

$$\frac{1}{2}\mathbf{v}(I + W) = \frac{1}{4}\mathbf{e}_1(-I + W)(I + W) = \frac{1}{4}\mathbf{e}_1(-(l + 1)I)$$

which lies in L. □

Let $\mathcal{I}$ be an ideal of $\mathcal{O}$. If M is a $\mathcal{O}$-module, then $\mathcal{I}M$, defined as the subgroup of M generated by the αm for $\alpha \in \mathcal{I}$ and $m \in M$, is also a $\mathcal{O}$-module.

Theorem 3.1 *Suppose that $l \equiv 7 \pmod 8$ and that $\mathcal{I}$ is a nonzero ideal of $\mathcal{O}$ with norm $N = N(\mathcal{I})$. If $L = L_+$ or L_- then*

$$L[\mathcal{I}] = \frac{1}{\sqrt{N}}\mathcal{I}L$$

is an even unimodular lattice. Also if $\mathcal{I}$ and $\mathcal{J}$ lie in the same ideal class of $\mathcal{O}$, the lattices $L[\mathcal{I}]$ and $L[\mathcal{J}]$ are isometric.

Proof First of all we show that the index $|L : \mathcal{I}L|$ equals $N^{n/2}$. As an $\mathcal{O}$-module, L is finitely generated. Also if $\alpha \in \mathcal{O}$ and $\mathbf{v} \in L$ are nonzero, then $|\alpha\mathbf{v}| = |\alpha||\mathbf{v}| \neq 0$ by Lemma 2.1 and so L is torsion free as an $\mathcal{O}$-module.

By the theory of modules over Dedekind domains [4, §9.6], as L is a finitely generated torsion-free module over the Dedekind domain $\mathcal{O}$, then $L = L_1 \oplus \cdots \oplus L_k$ where each L_j is isomorphic to a nonzero ideal $\mathcal{A}_j$ of $\mathcal{O}$.

Each of the $\mathcal{A}_j$ is a free abelian group of rank 2, and as L is a free abelian group of rank n it follows that $k = n/2$. Then $\mathcal{I}L = \mathcal{I}L_1 \oplus \cdots \oplus \mathcal{I}L_{n/2}$ and so $|L : \mathcal{I}L| = \prod_{j=1}^{n/2} |L_j : \mathcal{I}L_j|$. But

$$|L_j : \mathcal{I}L_j| = |\mathcal{A}_j : \mathcal{I}\mathcal{A}_j| = \frac{|\mathcal{O} : \mathcal{I}\mathcal{A}_j|}{|\mathcal{O} : \mathcal{A}_j|} = \frac{N(\mathcal{I}\mathcal{A}_j)}{N(\mathcal{A}_j)}.$$

But $N(\mathcal{I}\mathcal{A}_j) = N(\mathcal{I})N(\mathcal{A}_j)$ and so $|L_j : \mathcal{I}L_j| = N(\mathcal{I}) = N$. Consequently $|L : \mathcal{I}L| = N^{n/2}$ as claimed.

We now show that $L[\mathcal{I}]$ is unimodular. The lattice $\mathcal{I}L$ is generated by elements $\mathbf{u} = \alpha\mathbf{v}$ where $\alpha \in \mathcal{I}$ and $\mathbf{v} \in L$. Let $\mathbf{u}_j = \alpha_j\mathbf{v}_j$ $(j = 1, 2)$ with $\alpha_j \in \mathcal{I}$ and $\mathbf{v}_j \in L$. Then by Lemma 2.1,

$$\mathbf{u}_1 \cdot \mathbf{u}_2 = (\alpha_1\mathbf{v}_1) \cdot (\alpha_2\mathbf{v}_2) = (\alpha_1\alpha_2^*\mathbf{v}_1) \cdot \mathbf{v}_2.$$

But $\alpha_1\alpha_2^* \in \mathcal{I}\mathcal{I}^* = N(\mathcal{I})\mathcal{O}$ [3, §VIII.1] so that.

$$\mathbf{u}_1 \cdot \mathbf{u}_2 = N(\gamma\mathbf{v}_1) \cdot \mathbf{v}_2$$

where $\gamma \in \mathcal{O}$. As $\gamma\mathbf{v}_1 \in L$ (by Lemma 3.2) and L is an integral lattice, then $\mathbf{u}_i \cdot \mathbf{u}_2 \equiv 0 \pmod N$. Consequently $L[\mathcal{I}] = N^{-1/2}\mathcal{I}L$ is an integral lattice. But L is unimodular, so it has volume 1. Thus $\mathcal{I}L$ has volume $|L : \mathcal{I}L| = N^{n/2}$ and so $L[\mathcal{I}] = N^{-1/2}\mathcal{I}L$ has volume 1. Thus $L[\mathcal{I}]$ is a unimodular lattice.

We finally show that $L[\mathcal{I}]$ is an even unimodular lattice. Since $L[\mathcal{I}]$ is integral, to show that it is even it suffices to show that each vector $\mathbf{u}$ in a generating set of $L[\mathcal{I}]$ has $|\mathbf{u}|^2$ even. The vectors $\mathbf{u} = N^{-1/2}\alpha\mathbf{v}$ for $\alpha \in \mathcal{I}$ and $\mathbf{v} \in L$ generate $L[\mathcal{I}]$. Then

$$|\mathbf{u}|^2 = \frac{1}{N}|\alpha\mathbf{v}|^2 = \frac{|\alpha|^2}{N}|\mathbf{v}|^2.$$

But $|\alpha^2| = \alpha\alpha^* \in \mathcal{I}\mathcal{I}^* = N\mathcal{O}$ and so $|\alpha|^2/N \in \mathbf{Q} \cap \mathcal{O} = \mathbf{Z}$ and $|\mathbf{v}|^2$ is an even integer, as $\mathbf{v} \in L$, an even lattice. Thus $|\mathbf{u}|^2$ is an even integer. Thus $L[\mathcal{I}]$ is an even unimodular lattice.

Now suppose that $\mathcal{I}$ and $\mathcal{J}$ lie in the same ideal class of $\mathcal{O}$. Then $\mathcal{J} = \alpha\mathcal{I}$ where α is a nonzero element of K. Then $\mathcal{J}L = \alpha\mathcal{J}_L$ and so

$$L[\mathcal{J}] = \frac{1}{\sqrt{N(\mathcal{J})}}\mathcal{J}L = \frac{1}{\sqrt{N(\mathcal{J})}}\alpha\mathcal{I}L = \sqrt{\frac{N(\mathcal{I})}{N(\mathcal{J})}}\alpha L[\mathcal{I}].$$

Let $\gamma = \alpha\sqrt{N(\mathcal{I})/N(\mathcal{J})}$. Since $\mathcal{J} = \alpha\mathcal{I}$ then $N(\mathcal{J}) = |\alpha|^2 N(\mathcal{I})$ and so $|\gamma| = 1$. By Lemma 2.1, the map $\mathbf{v} \mapsto \gamma\mathbf{v}$ is an isometry of $\mathbf{R}^n$ and as $L[\mathcal{J}] = \gamma L[\mathcal{I}]$, the lattices $L[\mathcal{I}]$ and $L[\mathcal{J}]$ are isometric. $\square$

Given L, we can produce a maximum of h non-isometric lattices $L[\mathcal{I}]$ where h denotes the class-number of the quadratic field K.

It is useful to note which for which ideals $\mathcal{I}$ is $\mathcal{I}L_+ \subseteq \mathbf{Z}^n$.

Lemma 3.3 *Let $\mathcal{I}$ be an ideal of $\mathcal{O}$. Then $\mathcal{I}L_+ \subseteq \mathbf{Z}^n$ if and only if $\mathcal{I} \subseteq \left\langle 2, \frac{1}{2}(1-\sqrt{-l})\right\rangle$. In this case also $N(\mathcal{I})\mathbf{Z}^n \subseteq \mathcal{I}L_+$.*

Proof Note that $L_+ \cap \mathbf{Z}^n = L_0$ and so $\mathcal{I}L_+ \subseteq \mathbf{Z}^n$ if and only if $\mathcal{I}L_+ \subseteq L_0$. This occurs if and only if $\mathcal{I}$ annihilates the $\mathcal{O}$-module $M = L_+/L_0$. This module has 2 elements, so it must be isomorphic to $\mathcal{O}/\mathcal{J}$ where $\mathcal{J}$ is an ideal of norm 2. As $\left\langle 2, \frac{1}{2}(1-\sqrt{-l})\right\rangle$ has norm 2 and is seen to annihilate M as $\frac{1}{2}(1-\sqrt{-l})$ takes $\frac{1}{2}\mathbf{e}_1(I+W)$ to $\frac{1}{4}(l+1)\mathbf{e}_1$, then $\mathcal{J} = \left\langle 2, \frac{1}{2}(1-\sqrt{-l})\right\rangle$. Thus $\mathcal{J}$ is the annihilator of M and the first statement follows.

Suppose that $\mathcal{I} \subseteq \left\langle 2, \frac{1}{2}(1-\sqrt{-l})\right\rangle$. The lattice $L_+[\mathcal{I}]$ is unimodular so that if $\mathbf{u}\cdot\mathbf{v} \in \mathbf{Z}$ for all $\mathbf{v} \in L_+[\mathcal{I}]$ then $\mathbf{u} \in L_+[\mathcal{I}]$. If $\mathbf{u} = \sqrt{N(\mathcal{I})}\mathbf{w}$ with $\mathbf{w} \in \mathbf{Z}^n$ then $\mathbf{u}\cdot\mathbf{v} \in \mathbf{Z}$ for all $\mathbf{v} \in N(\mathcal{I})^{-1/2}\mathbf{Z}^n$ and as $L_+[\mathcal{I}] \subseteq N(\mathcal{I})^{-1/2}\mathbf{Z}^n$ then $\mathbf{u} \in L_+[\mathcal{I}]$. Hence $\sqrt{N(\mathcal{I})}\mathbf{Z}^n \subseteq L_+[\mathcal{I}]$ and so $N(\mathcal{I})\mathbf{Z}^n \subseteq \mathcal{I}L_+$. $\square$

In this case the lattice Λ is the inverse image of a subgroup $\mathcal{C}$ of $(\mathbf{Z}/N\mathbf{Z})^n$, where $N = N(\mathcal{I})$, under the projection $\pi : \mathbf{Z}^n \to (\mathbf{Z}/N\mathbf{Z})^n$. Such a subgroup is called a *linear code* of length n over $\mathbf{Z}/N\mathbf{Z}$. We also say that Λ is obtained from $\mathcal{C}$ by *construction A_N*.

The standard dot product is well-defined on the group $(\mathbf{Z}/N\mathbf{Z})^n$. If a subgroup $\mathcal{C} \subseteq (\mathbf{Z}/N\mathbf{Z})^n$ satisfies $\mathbf{u}\cdot\mathbf{v} = 0$ for all $\mathbf{u}$, $\mathbf{v} \in \mathcal{C}$ then $\mathcal{C}$ is *self-orthogonal*. Also $\mathcal{C}$ is *self-dual* if $\mathbf{u}\cdot\mathcal{C} = 0$ if and only if $\mathbf{u} \in \mathcal{C}$. By the nondegeneracy of the dot product, $\mathcal{C}$ is self-dual if and only if $\mathcal{C}$ is self-orthogonal and $|\mathcal{C}| = N^{n/2}$.

Proposition 3.1 *Let $\mathcal{I}$ be an ideal of $\mathcal{O}$ with $\mathcal{I} \subseteq \left\langle 2, \frac{1}{2}(1-\sqrt{-l})\right\rangle$ and $N(\mathcal{I}) = N$. The lattice $L = \mathcal{I}L_+$ is obtained from construction A_N from a self-dual linear code $\mathcal{C}$ of length n over $\mathbf{Z}/N\mathbf{Z}$.*

If $\mathcal{I} = \left\langle N, \frac{1}{2}(a-\sqrt{-l})\right\rangle$ with $a \equiv 1 \pmod 4$ and $a^2 \equiv -l \pmod{4N}$ then $\mathcal{C}$ is spanned by the vectors of the form $\frac{1}{2}(\mathbf{e}_i + \mathbf{e}_j)(aI - W)$ $(1 \le i \le j \le n)$.

Proof Apart from the self-duality of $\mathcal{C}$ we have already proved the first assertion. The self-duality of $\mathcal{C}$ follows from the unimodularity of $N^{-1/2}\mathcal{I}L_+$. By volume considerations

$$N^{n/2} = |\mathbf{Z}^n : \mathcal{I}L_+| = |(\mathbf{Z}/N\mathbf{Z})^n : \mathcal{C}|$$

and so $|\mathcal{C}| = N^{n/2}$. Also if $\mathbf{u}$, $\mathbf{v} \in \mathcal{I}L_+$ then $N^{-1/2}\mathbf{u}$ and $N^{-1/2}\mathbf{v}$ lie in the integral lattice $N^{-1/2}\mathcal{I}L_+$ so that $N^{-1}\mathbf{u}\cdot\mathbf{v} \in \mathbf{Z}$. Hence $\mathcal{C}$ is self-orthogonal, and as it has the correct order, it is self-dual.

The ideal $\mathcal{I}$ contains the subgroup $N\mathbf{Z} + \frac{1}{2}(a - \sqrt{-l})\mathbf{Z}$ of $\mathcal{O}$ and as this subgroup also has index N in $\mathcal{O}$ then $\mathcal{I} = N\mathbf{Z} + \frac{1}{2}(a - \sqrt{-l})\mathbf{Z}$. It follows that $\mathcal{I}L_+ = NL_+ + \frac{1}{2}(a - \sqrt{-l})L_+$. As $a \equiv 1 \pmod 4$, $\frac{1}{2}(a + \sqrt{-l}) - \frac{1}{2}(1 + \sqrt{-l})$ is an even integer. It follows that $L_0 + \frac{1}{2}\mathbf{e}_1(aI + W) = L_0 + \frac{1}{2}\mathbf{e}_1(I + W)$ and so L_+ is generated by L_0 and $\mathbf{u} = \frac{1}{2}\mathbf{e}_1(aI + W)$. Thus NL_+ is generated by the $N(\mathbf{e}_i + \mathbf{e}_j)$ and $N\mathbf{u}$ and $\frac{1}{2}(a - \sqrt{-l})L_+$ is generated by the $\frac{1}{2}(\mathbf{e}_i + \mathbf{e}_j)(aI - W)$ and

$$\frac{1}{2}\mathbf{u}(aI - W) = \frac{1}{4}\mathbf{e}_1(aI - W)(aI + W) = \frac{a^2 + l}{4}.$$

Note that $(a^2 + l)/4$ is a multiple of N. It follows that $\mathcal{C}$ is generated by $N\mathbf{u}$ and the $\frac{1}{2}(\mathbf{e}_i + \mathbf{e}_j)(aI - W)$. But $N\mathbf{u} = (N/2)\mathbf{e}_1(I + W)$ is congruent modulo N to the word consisting of all $N/2$s. Also $(N/2)\mathbf{e}_1(aI - W)$ is congruent to the same word. We can drop the generator $N\mathbf{u}$ and deduce that $\mathcal{C}$ is generated by the $\frac{1}{2}(\mathbf{e}_i + \mathbf{e}_j)(aI - W)$. $\square$

4 Quadratic residue codes

To use the above construction of lattices, we need a supply of skew-symmetric conference matrices. Paley [8] constructed a family of such matrices of order $n = l + 1$ whenever $l \equiv 3 \pmod 4$ is prime. To apply our theory we stipulate in addition that $l \equiv 7 \pmod 8$. We find that the lattices $\mathcal{I}L_+$ are derived from quadratic residue codes in this case.

We define a conference matrix $W \in \mathcal{W}_n$ as follows. Let

$$W = \begin{pmatrix} 0 & 1 & \cdots & 1 \\ -1 & & & \\ \vdots & & W' & \\ -1 & & & \end{pmatrix}$$

where the l-by-l matrix W' is the circulant matrix whose (i, j)-entry is

$$W'_{ij} = \left(\frac{j - i}{l}\right)$$

where $\left(-\right)$ denotes the Legendre symbol. This matrix W is called a conference matrix of *Paley type*. For the rest of this section W will denote this particular matrix.

We follow the usual practice with quadratic residue codes and label the entries of a typical vector of length $n = l + 1$ using the elements of the projective line over $\mathbf{F}_l$ as follows: $\mathbf{v} = (v_\infty, v_0, v_1, v_2, \ldots, v_{l-1})$. We let $\mathbf{e}_\infty$, $\mathbf{e}_0$, $\mathbf{e}_1, \ldots \mathbf{e}_{l-1}$ denote the corresponding unit vectors, that is, $\mathbf{e}_\mu$ has a one in the position labelled μ, and zeros elsewhere.

Lemma 4.1 (Paley) *The matrix W is a skew-symmetric conference matrix.*

Proof See for instance [7, Chapter 18]. $\square$

In $\mathcal{O}$, the ideal $2\mathcal{O}$ splits as a product of two distinct prime ideals: $2\mathcal{O} = \mathcal{P}\mathcal{Q}$ where $\mathcal{P} = \left\langle 2, \frac{1}{2}(1+\sqrt{-l})\right\rangle$ and $\mathcal{Q} = \mathcal{P}^* = \left\langle 2, \frac{1}{2}(1-\sqrt{-l})\right\rangle$. We shall investigate the lattices $L_+[\mathcal{P}^r]$ and $L_+[\mathcal{Q}^r]$ for integers $r \geq 0$. (The discussion for $L_-[\mathcal{P}^r]$ and $L_-[\mathcal{Q}^r]$ is similar.)

We first need a lemma on the structure of the ideals $\mathcal{P}^r$ and $\mathcal{Q}^r$.

Lemma 4.2 *Let r be a positive integer. Then*

$$\mathcal{P}^r = 2^r\mathbf{Z} + \frac{1}{2}(t+\sqrt{-l})\mathbf{Z}$$

and

$$\mathcal{Q}^r = 2^r\mathbf{Z} + \frac{1}{2}(t-\sqrt{-l})\mathbf{Z}$$

where t is any integer with $t^2 \equiv -l \pmod{2^{r+2}}$ and $t \equiv 1 \pmod 4$.

Proof It is well-known that if $s \geq 3$, and $a \equiv 1 \pmod 8$ then the congruence $x^2 \equiv a \pmod{2^s}$ is soluble. Thus there exists t with $t^2 \equiv -l \pmod{2^{r+2}}$. By replacing t by $-t$ if necessary, we may assume that $t \equiv 1 \pmod 4$. Consider the ideal $\mathcal{I} = \left\langle 2^r, \frac{1}{2}(t+\sqrt{-l})\right\rangle$ of $\mathcal{O}$. As $2^r \in \mathcal{I}$ then $\mathcal{I}$ is a factor of $2^r\mathcal{O} = \mathcal{P}^r\mathcal{Q}^r$. But as $\frac{1}{2}(t+\sqrt{-l}) = \frac{1}{2}(1+\sqrt{-l}) + 2(t-1)/4 \in \mathcal{P}$ then $\mathcal{P}$ is a factor of $\mathcal{I}$. But $\frac{1}{4}(t+\sqrt{-l}) \notin \mathcal{O}$, and so $2\mathcal{O}_K = \mathcal{P}\mathcal{Q}$ is not a factor of $\mathcal{I}$. Hence $\mathcal{I} = \mathcal{P}^{r'}$ where $1 \leq r' \leq r$. Letting $\alpha = \frac{1}{2}(t+\sqrt{-l})$ we have

$$\begin{aligned}
\mathcal{I}\mathcal{I}^* &= \langle 2^r, \alpha\rangle \langle 2^r, \alpha^*\rangle \\
&= \left\langle 2^{2r}, 2^r\alpha, 2^r\alpha^*, \alpha\alpha^*\right\rangle \\
&= \left\langle 2^{2r}, 2^r\alpha, 2^r\alpha^*, (t^2+l)/4\right\rangle \\
&\subseteq 2^r\mathcal{O}
\end{aligned}$$

as $t^2 \equiv -l \pmod{2^{r+2}}$. But $\mathcal{I}\mathcal{I}^* = N(\mathcal{I})\mathcal{O} = 2^{r'}\mathcal{O}$ and so $r = r'$, that is $\mathcal{I} = \mathcal{P}^r$.

Now $\mathcal{P}^r \subseteq 2^r\mathbf{Z} + \frac{1}{2}(t+\sqrt{-l})\mathbf{Z}$, but both these groups have index 2^r in $\mathcal{O}$ so they are equal. The statement about $\mathcal{Q}^r$ now follows by complex conjugation. $\square$

We now consider the lattices $\mathcal{Q}^rL_+$ for $r \geq 1$. Since $\mathcal{Q}^r \subseteq \mathcal{Q}$ and $\mathcal{Q} = \left\langle 2, \frac{1}{2}(1-\sqrt{-l})\right\rangle$ then by Proposition 3.1 $\mathcal{Q}^rL_+$ is obtained by construction A_{2^r} from a self-dual code $\mathcal{C}_r$ over $\mathbf{Z}/2^r\mathbf{Z}$. We shall show that $\mathcal{C}_r$ is the Hensel lift of an extended quadratic residue code in the sense of [1].

Recall that the integer t satisfies $t \equiv 1 \pmod 4$ and $t^2 \equiv -l \pmod{2^{r+2}}$. By Proposition 3.1 it follows that $\mathcal{C}_r$ is generated by the vectors $\frac{1}{2}(\mathbf{e}_i + \mathbf{e}_j)(W - tI)$. It is plain that we need only these vectors with $i = \infty$ and so $\mathcal{C}_r$ is spanned by $\mathbf{u} = \mathbf{e}_\infty(W - tI)$ and $\mathbf{v}_j = \frac{1}{2}(\mathbf{e}_\infty + \mathbf{e}_j)(W - tI)$ for $0 \le j < l$.

Let $\phi : (\mathbf{Z}/2^r\mathbf{Z})^n \to (\mathbf{Z}/2^r\mathbf{Z})^l$ be the map given by deleting the first coordinate of the vector. The code $\mathcal{C}_r$ contains the vector $\mathbf{u} = (-t, 1, 1, \ldots, 1)$. As r is odd and $\mathcal{C}_r$ is self-dual, the intersection of $\mathcal{C}_r$ and the kernel of ϕ is trivial. Thus $\mathcal{C}'_r = \phi(\mathcal{C}_r)$ has the same order as $\mathcal{C}_r$. Then $\phi(\mathbf{u})$ is the all-ones vector, and $\phi(\mathbf{v}_j)$ are cyclic shifts of $\phi(\mathbf{v}_0)$. Also $\phi(\mathbf{v}_0) = (c_0, c_1, \ldots, c_{p-1})$ where

$$c_j = \begin{cases} (1-t)/2 & \text{if } j = 0, \\ 1 & \text{if } j \text{ is a quadratic residue modulo } l, \\ 0 & \text{if } j \text{ is a quadratic nonresidue modulo } l. \end{cases}$$

Thus $\mathcal{C}'_r$ is a cyclic code over $\mathbf{Z}/2^r\mathbf{Z}$.

We recall the definition of quadratic residue codes. Consider the polynomial $X^l - 1$ over the field $\mathbf{F}_2 = \mathbf{Z}/2\mathbf{Z}$. Then $X^l - 1$ splits into linear factors in some finite extension $\mathbf{F}_{2^k}$ of $\mathbf{F}_2$. In fact

$$X^l - 1 = \prod_{j=0}^{l-1}(X - \zeta^j)$$

where ζ is a primitive l-th root of unity in $\mathbf{F}_{2^k}$. We write

$$X^l - 1 = (X-1)f_+(X)f_-(X)$$

where

$$f_+(X) = \prod_{(j/l)=1}(X - \zeta^j) \quad \text{and} \quad f_-(X) = \prod_{(j/l)=-1}(X - \zeta^j).$$

As $l \equiv 7 \pmod 8$, then 2 is a quadratic residue modulo l, and so the coefficients of both f_+ and f_- are invariant under the Frobenius automorphism $\delta \mapsto \delta^2$ of $\mathbf{F}_{2^k}$. Consequently both f_+ and f_- have coefficients in $\mathbf{F}_2$. The labelling of these factors as f_+ and f_- depends on the choice of ζ. Replacing ζ by another primitive l-th root of unity either preserves or interchanges f_+ and f_-. The coefficients of $X^{(l-3)/2}$ in f_+ and f_- are 0 and 1 is some order, so we can, and shall, choose ζ such that

$$f_+(X) = X^{(l-1)/2} + 0X^{(l-3)/2} + \cdots \quad \text{and} \quad f_-(X) = X^{(l-1)/2} + X^{(l-3)/2} + \cdots.$$

The cyclic codes of length l over $\mathbf{F}_2$ with generator polynomials $f_+(X)$ and $f_-(X)$ are called the quadratic residue codes.

Bonnecaze, Solé and Calderbank [1] extended the notion of quadratic residue code to codes over $\mathbf{Z}/2^r\mathbf{Z}$. By Hensel's lemma there exist unique polynomials $f_+^{(r)}(X)$ and $f_-^{(r)}(X)$ with coefficients in $\mathbf{Z}/2^r\mathbf{Z}$ such that

$$X^l - 1 = (X-1)f_+^{(r)}(X)f_-^{(r)}(X),$$

$$f_+^{(r)}(X) \equiv f_+(X) \pmod 2 \quad \text{and} \quad f_-^{(r)}(X) \equiv f_-(X) \pmod 2.$$

The cyclic codes over $\mathbf{Z}^l$ with generator polynomials $f_+^{(r)}(X)$ and $f_-^{(r)}(X)$ are called lifted quadratic residue codes over $\mathbf{Z}/2^r\mathbf{Z}$.

Theorem 4.1 *The code $\mathcal{C}'_r$ is the lifted quadratic residue code over $\mathbf{Z}/2^r\mathbf{Z}$ with generator polynomial $f_+^{(r)}(X)$.*

Proof Cyclic codes of length l over $R = \mathbf{Z}/2^r\mathbf{Z}$ correspond to ideals of the polynomial ring $R[X]/\left\langle X^l - 1\right\rangle$. The code $\mathcal{C}'_r$ corresponds to the ideal $\mathcal{I} = \langle g, h\rangle$ where

$$g(X) = \sum_{j=0}^{p-1} X^j$$

and

$$h(X) = \frac{1-t}{2} + \sum_{(j/l)=1} X^j.$$

We first consider the case where $r = 1$. Then $\mathcal{I} = \langle u(X)\rangle$ where $u(X)$ is the greatest common divisor of $g(X)$ and $h(X)$. Let ζ be a root of $f_+(X) = 0$ in an extension field of $\mathbf{F}_2$. The roots of $g(X)$ are the ζ^j where $p \nmid j$. As $t \equiv 1 \pmod 4$ then $\frac{1}{2}(1-t)$ is even and so $h(X) = \sum_{(j/l)=1} X^j$. Now

$$\sum_{(j/l)=1} \zeta^j = 0 \qquad \text{and} \qquad \sum_{(j/l)=-1} \zeta^j = 1.$$

It follows that

$$h(\zeta^a) = \sum_{(j/l)=1} (\zeta^a)^j = 0$$

if and only if $\left(\frac{a}{l}\right) = 1$. Thus $u(X) = f_+(X)$.

Now we consider the general case. The reduction of $\mathcal{C}'_r$ modulo 2 is $\mathcal{C}'_1$. Any liftings to $\mathcal{C}'_r$ of a basis of $\mathcal{C}'_1$ generate a free R-module (of rank $\frac{1}{2}(l+1)$), and so they generate the whole code $\mathcal{C}'_r$. As $\mathcal{C}_r$ is free over R, it is generated as an ideal by a monic polynomial $F(X)$, of degree $\frac{1}{2}(l+1)$. As $F(X)$ reduces to $f_+(X)$ modulo 2, and $F(X) \mid X^l - 1$ it follows that $F(X) = f_+^{(r)}(X)$ as required. $\square$

Given the code $\mathcal{C}_r'$, the code $\mathcal{C}_r$ can be reconstructed, since for each element of $\mathcal{C}_r'$ the corresponding element of $\mathcal{C}_r$ is uniquely determined as it is orthogonal to $(-t, 1, 1, \ldots, 1)$.

We now turn to $\mathcal{P}^r L_+$. This is no longer a sublattice of $\mathbf{Z}^n$.

Lemma 4.3 *Let r be a positive integer. The index $|\mathcal{P}^r L_+ : \mathcal{P}^r L_+ \cap \mathbf{Z}^n| = 2$. The lattice $\mathcal{P}^r L_+ \cap \mathbf{Z}^n$ is generated by the vectors $2^r(\mathbf{e}_\infty + \mathbf{e}_\mu)$ ($\mu \in \{\infty, 0, 1, 2, \ldots, l-1\}$), the vector $\mathbf{u} = \mathbf{e}_\infty(W + tI)$ and and the vectors $\mathbf{v}_j = \frac{1}{2}(\mathbf{e}_\infty + \mathbf{e}_j)(W + tI)$ ($0 \le j < l$). Also $\mathcal{P}^r L_+$ is generated by $\mathcal{P}^r L_+ \cap \mathbf{Z}^n$ and $\frac{1}{2}\mathbf{u} - \frac{1}{4}(t^2 + l)\mathbf{e}_\infty$.*

Proof We have $\mathcal{P}^r = 2^r\mathbf{Z} + \frac{1}{2}(t + \sqrt{-l})\mathbf{Z}$. Let Ω_0 denote the lattice generated by the $2^r(\mathbf{e}_\infty + \mathbf{e}_\mu)$, $\mathbf{u}$ and the $\mathbf{v}_j$. The lattice L_+ is generated by the $\mathbf{e}_\infty + \mathbf{e}_\mu$ and $\frac{1}{2}\mathbf{e}_\infty(tI + W)$. Thus $2^r(\mathbf{e}_\infty + \mathbf{e}_\mu)$, $\mathbf{u} = \frac{1}{2}(t + \sqrt{-l})2\mathbf{e}_\infty$ and $\mathbf{v}_j = \frac{1}{2}(t + \sqrt{-l})(\mathbf{e}_\infty + \mathbf{e}_j)$ all lie in $\mathcal{P}^r L_+$. These vectors all have integer coordinates, and so $\Omega_0 \subseteq \mathcal{P}^r L_+ \cap \mathbf{Z}^n$.

Let Ω be the lattice generated by Ω_0 and $\frac{1}{2}\mathbf{u} - \frac{1}{4}(t^2 + l)\mathbf{e}_\infty$. Now

$$\begin{aligned}
\frac{1}{2}(t + \sqrt{-l})\frac{1}{2}\mathbf{e}_\infty(tI + W) &= \frac{1}{4}(t + \sqrt{-l})^2\mathbf{e}_\infty \\
&= \left[\frac{t}{2}(t + \sqrt{-l}) - \frac{t^2 + l}{4}\right]\mathbf{e}_\infty \\
&= \frac{t}{2}\mathbf{u} - \frac{t^2 + l}{4}\mathbf{e}_\infty.
\end{aligned}$$

As t is odd and $\mathbf{u} \in \Omega_0$ then $\Omega \subseteq \mathcal{P}^r L_+$.

The lattice $\mathcal{P}^r L_+$ is generated by Ω and $2^{r-1}\mathbf{e}_\infty(tI + W) = 2^{r-1}\mathbf{u}$. But $\mathbf{u} - \frac{1}{2}(t^2 + l)\mathbf{e}_\infty \in \Omega$ and as $t^2 + l$ is divisible by 2^{r+1} then $\mathbf{u} \in \Omega_0$ and so $\Omega = \mathcal{P}^r L_+$. As $\frac{1}{2}\mathbf{u} - \frac{1}{4}(t^2 + l)\mathbf{e}_\infty$ is not in $\mathbf{Z}^n$ but its double is in Ω_0, then $|\Omega : \Omega_0| = |\mathcal{P}^r L_+ : \mathcal{P}^r L_+ \cap \mathbf{Z}^n| = 2$ and so $\Omega_0 = \mathcal{P}^r L_+ \cap \mathbf{Z}^n$. $\square$

One can now proceed to express the lattices $\mathcal{P}^r L_+$ and $\mathcal{P}^r L_+ \cap \mathbf{Z}^n$ in terms of lifted quadratic residue codes over $\mathbf{Z}/2^r\mathbf{Z}$. For simplicity we present the details only for $r = 1$. Let $\mathcal{D}'$ denote the cyclic quadratic residue code of length l over $\mathbf{F}_2$ with generator polynomial $f_-(X)$, and let $\mathcal{D}$ denote its extension obtained by appending a parity check bit at the front.

Theorem 4.2 *The lattice $\mathcal{P}L_+ \cap \mathbf{Z}^n$ consists of those vectors reducing modulo 2 to elements of $\mathcal{D}$ and the sum of whose entries is a multiple of 4. The lattice $\mathcal{P}L_+$ is obtained from $\mathcal{P}L_+ \cap \mathbf{Z}^n$ by adjoining the extra generator $\frac{1}{2}(\frac{1}{2}(1 - l), 1, 1, \ldots, 1)$.*

Proof We may take $t = 1$ in the proof of Lemma 4.3. In this case the vector $\mathbf{u}$ is the all-ones vector while each $\mathbf{v}_j$ consists of $\frac{1}{2}(l+1)$ ones and $\frac{1}{2}(l+1)$ zeros. As $\frac{1}{2}(l+1)$ is a multiple of 4 the sum of the entries of each of these vectors is a multiple of 4. As this is manifestly true for the vectors $2(\mathbf{e}_\infty + \mathbf{e}_\mu)$ too, then the sum of the entries of each vector in $\mathcal{P}L_+ \cap \mathbf{Z}^n$ is a multiple of 4.

If we delete the first entry of the given generators of $\mathcal{P}L_+$ and reduce modulo 2 we get the all-ones vector of length l and the cyclic shifts of the vector $\mathbf{w}_0 = (d_0, d_1, \ldots, d_{l-1})$ where

$$d_j = \begin{cases} 1 & \text{if } j = 0 \text{ or if } j \text{ is a quadratic residue modulo } l, \\ 0 & \text{if } j \text{ is a quadratic nonresidue modulo } l. \end{cases}$$

By a similar argument to the proof of Theorem 4.1 these vectors generate the cyclic quadratic residue code $\mathcal{D}'$. Hence each element of $\mathcal{P}L_+ \cap \mathbf{Z}^n$ reduces modulo 2 to an element of $\mathcal{D}$. If Ω denotes the sublattice of $\mathbf{Z}^n$ consisting of vectors reducing modulo 2 to $\mathcal{D}$ and with the entries summing to a multiple of 4, then $|\mathbf{Z}^n : \Omega| = 2^{1+n/2} = |\mathbf{Z}^n : \mathcal{P}L_+ \cap \mathbf{Z}^n|$. Thus $\Omega = \mathcal{P}L_+ \cap \mathbf{Z}^n$.

Now letting $t = 1$ we see that $\frac{1}{2}\mathbf{u} - \frac{1}{4}(t^2 + l)\mathbf{e}_\infty = \frac{1}{2}(\frac{1}{2}(1-l), 1, 1, \ldots, 1)$ and so this vector together with $\mathcal{P}L_+ \cap \mathbf{Z}^n$ generates $\mathcal{P}L_+$. □

In the terminology of Conway and Sloane [5, Chapter 5, §3], the lattice $\mathcal{P}L_+ \cap \mathbf{Z}^n$ is obtained from the code $\mathcal{D}$ by construction B. Then the lattice $\mathcal{P}L_+$ is obtained by density doubling. One can extend these notions to lifted quadratic residue codes to produce the lattices $\mathcal{P}^r L_+$.

We look briefly at the lattices $\mathcal{I}L_+$ for more general ideals $\mathcal{I}$. Consider the case where $\mathcal{I} = \mathcal{A}$, an ideal of norm p, an odd prime. Then $\mathcal{A} = \langle p, t + \sqrt{-l} \rangle$ where $t^2 \equiv -l \pmod p$. The rows of the matrix $tI + W$ generate a self-dual linear code $\mathcal{C}$ over $\mathbf{F}_p$ which turns out to be an extended quadratic residue code. The coordinates of vectors in L_+ are half-integers, and it is meaningful to reduce these modulo the odd prime p. Then the lattice $\mathcal{A}L_+$ simply consists of the vectors in L_+ which reduce modulo p to elements of $\mathcal{C}$. More generally $\mathcal{A}^r L_+$ will have a similar description in terms of an extended lifted quadratic residue code over $\mathbf{Z}/p^r\mathbf{Z}$. Finally by splitting a general ideal $\mathcal{I}$ into a product of powers of prime ideals $\mathcal{A}^r$, we can describe $\mathcal{I}L_+$ in terms of the various $\mathcal{A}^r$ using the Chinese remainder theorem.

5 Examples

Since the ring $\mathbf{Z}[\frac{1}{2}(1 + \sqrt{-7})]$ has class number 1 (and each even unimodular rank 8 lattice is isometric to the E_8 root lattice) the first interesting examples

occur when $l = 15$ and the first interesting examples with Paley matrices occur when $l = 23$.

5.1 $l = 23$ and $l = 31$

In both these cases we take W to be the Paley matrix. We first consider the case $l = 23$.

The class group of $\mathcal{O} = \mathbf{Z}[\frac{1}{2}(1+\sqrt{-23})]$ has order 3, and the class of each of its ideals $\mathcal{P} = \left\langle 2, \frac{1}{2}(1+\sqrt{-23})\right\rangle$ and $\mathcal{Q} = \left\langle 2, \frac{1}{2}(1-\sqrt{-23})\right\rangle$ generates its class group. The lattice L_+ itself is the lattice D_{24}^+. The lattices $\mathcal{Q}^r L_+$ are obtained by applying construction A_{2^r} to the lifted quadratic residue codes $\mathcal{C}_r$. The code $\mathcal{C}_1$ is the extended binary Golay code. It is plain that $\mathcal{Q}L_+$ is obtained by applying construction A [Chapter 5, §2] to the binary Golay code, and so $L_+[\mathcal{Q}]$ is isometric to the Niemeier lattice with root system A_1^{24}.

The isometry classes of the unimodular lattices $L_+[\mathcal{Q}^r]$ depend only on the congruence class of r modulo 3. If $r \equiv 0 \pmod 3$ then $L_+[\mathcal{Q}^r]$ is isometric to D_{24}^+ while if $r \equiv 1 \pmod 3$ then $L_+[\mathcal{Q}^r]$ is isometric to the Niemeier lattice with root system A_1^{24}. To identify $L_+[\mathcal{Q}^r]$ when $r \equiv 2 \pmod 3$ note that $\mathcal{Q}^2$ lies in the same ideal class as $\mathcal{P}$. Hence for $r \equiv 2 \pmod 3$, $L_+[\mathcal{Q}^r]$ is isometric to $L_+[\mathcal{P}]$. By Theorem 4.2 it is plain that $L_+[\mathcal{P}]$ is the Leech lattice, as given by Leech's original construction [6]. Applying Theorem 3.1 gives an explicit isomorphism between $L_+[\mathcal{P}]$ and $L_+[\mathcal{Q}^2]$ which is equivalent to that constructed in [2].

In general if s is the order of the class of the ideal $\mathcal{P}$ in the class group of $\mathcal{O}$, then up to isometry $L_+[\mathcal{P}^r]$ and $L_+[\mathcal{Q}^r]$ depend only on the congruence class of r modulo s. Also $L_+[\mathcal{P}^r]$ and $L_+[\mathcal{Q}^{r'}]$ will be isometric whenever $r \equiv -r' \pmod s$. For $l = 31$ we also have $s = 3$ and the above discussion is valid for $l = 31$ too. In particular $L_+[\mathcal{P}]$ is isometric to $L_+[\mathcal{Q}^2]$, and we recover [2, Theorem 1].

We can give alternative constructions of the Leech lattice at will simply by writing down ideals of $\mathbf{Z}[\frac{1}{2}(1+\sqrt{-23})]$ equivalent to $\mathcal{P}$. Let $\mathcal{I} = \left\langle 3, \frac{1}{2}(1+\sqrt{-23})\right\rangle$ and $\mathcal{J} = \left\langle 3, \frac{1}{2}(-1+\sqrt{-23})\right\rangle$. Then $\mathcal{P}$, $\mathcal{J}$ and $\mathcal{QI} = \left\langle 6, \frac{1}{2}(-5+\sqrt{-23})\right\rangle$ all lie in the same ideal class.

The lattice $\mathcal{J}L_+$ is generated using density doubling from the lattice L' consisting of all vectors in $\mathbf{Z}^{24}$ whose entries sum to zero and which reduce modulo 3 to elements of the extended ternary quadratic residue code with generator matrix $I - W$. Then $\mathcal{J}L_+$ is generated by L' and the vector $\frac{1}{2}(5, 1, 1, \ldots, 1)$. The lattice $L_+[\mathcal{J}] = 3^{-1/2}\mathcal{J}L_+$ is isometric to the Leech lattice.

Next consider the lattice $\mathcal{Q}\mathcal{I}L_+$. This consists of the vectors in $\mathbf{Z}^{24}$ reducing modulo 2 and modulo 3 to elements of appropriately chosen binary and ternary quadratic residue codes. The binary code in question is that generated by vectors $\frac{1}{2}(\mathbf{e}_\infty + \mathbf{e}_\alpha)(I - W)$ for $\alpha \in \{\infty, 0, 1, 2, \ldots, l-1\}$ and the ternary code is generated by the rows of $I + W$. Then $L_+[\mathcal{Q}\mathcal{I}] = 6^{-1/2}\mathcal{Q}\mathcal{I}L_+$ is isometric to the Leech lattice.

5.2 $l = 47$

Again we take W to be the Paley matrix. In [5, Chapter 7, §7] the lattice $\Lambda = P_{48q}$ is described. This is an even unimodular lattice of rank 48 and minimum norm 6. It is generated by the following vectors $(a_\infty, a_0, a_1, \ldots, a_{46})$:

(i) $(1/\sqrt{12})(-5, 1, 1, \ldots, 1)$,

(ii) those vectors of the shape $(1/\sqrt{3})(1^{24}, 0^{24})$ supported on the translates modulo 47 of the set $\{0\} \cup Q$ where Q is the set of quadratic residues modulo 47,

(iii) all vectors of the shape $(1/\sqrt{3})(\pm 3^2, 0^{46})$.

It is more convenient to consider instead the equivalent lattice Λ' generated by the vectors

(i)′ $(1/\sqrt{12})(5, 1, 1, \ldots, 1)$,

(ii)′ those vectors of the shape $(1/\sqrt{3})(1^{24}, 0^{24})$ supported on the translates modulo 47 of the set $\{0\} \cup N$ where N is the set of quadratic nonresidues modulo 47,

(iii)′ all vectors of the shape $(1/\sqrt{3})(\pm 3^2, 0^{46})$.

We claim that Λ' is the lattice $L_+[\mathcal{I}]$ where $\mathcal{I} = \left\langle 3, \frac{1}{2}(1 - \sqrt{-47})\right\rangle$. Note that the norm of $\mathcal{I}$ is 3. It suffices to show that each of the generating vectors for Λ' is contained in $L_+[\mathcal{I}]$. Since each vector of shape $(\pm 1^2, 0^{46})$ lies in L_+ and $3 \in P$ then it is immediate that the vectors of type (iii)′ lie in $L_+[\mathcal{I}]$. The vectors of type (ii)′ are the differences of the first row and an arbitrary other row of the matrix $(1/2\sqrt{3})(I - W)$. Since $\frac{1}{2}(1 - \sqrt{-47}) \in \mathcal{I}$, the vectors of type (ii)′ lie in $L_+[\mathcal{I}]$. Finally, $\frac{1}{2}(1, -1, -1, \ldots, -1)$, the first row of $\frac{1}{2}(I - W)$, lies in $\mathcal{I}L_+$. Also $\mathbf{v}_0 = \frac{1}{2}\mathbf{e}_0(I + W) \in L_+$ and $3\mathbf{v}_0 = \frac{1}{2}(3, 3, 3, \ldots, 3) \in \mathcal{I}L_+$. Adding these two vectors gives $\frac{1}{2}(5, 1, 1, \ldots, 1) \in \mathcal{I}L_+$ so that the vector of type (i)′ does lie in $L_+[\mathcal{I}]$.

The ideal $\left\langle \frac{1}{2}(1 - \sqrt{-47})\right\rangle$ has norm 12 and factors as $\mathcal{Q}^2\mathcal{I}$. The class number of $\mathbf{Q}(\sqrt{-47})$ is 5, and so $[\mathcal{I}] = [\mathcal{P}^2] = [\mathcal{Q}^3]$. Thus Λ' is isometric to

$L_+[\mathcal{Q}^3]$, which is constructed using construction A from the quadratic residue code of length 48 over $\mathbf{Z}/8\mathbf{Z}$.

5.3 $l = 15$

In this case there is no Paley matrix. We consider two different conference matrices of order 16.

If $W \in \mathcal{W}_n$ then the $2n$-by-$2n$ matrix

$$W' = \begin{pmatrix} W & I + W \\ -I + W & -W \end{pmatrix}$$

is a skew-symmetric conference matrix of order $2n$. Applying this construction four times to the zero matrix in $\mathcal{W}_1$ gives the matrix

$$W_1 = \left(\begin{array}{cccccccccccccccc}
0 & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + \\
- & 0 & - & + & - & + & - & + & - & + & - & + & - & + & - & + \\
- & + & 0 & - & - & + & + & - & - & + & + & - & - & + & + & - \\
- & - & + & 0 & - & - & + & + & - & - & + & + & - & - & + & + \\
- & + & + & + & 0 & - & - & - & - & + & + & + & + & - & - & - \\
- & - & - & + & + & 0 & + & - & - & - & - & + & + & + & + & - \\
- & + & - & - & + & - & 0 & + & - & + & - & - & + & - & + & + \\
- & - & + & - & + & + & - & 0 & - & - & + & - & + & + & - & + \\
- & + & + & + & + & + & + & + & 0 & - & - & - & - & - & - & - \\
- & - & - & + & - & + & - & + & + & 0 & + & - & + & - & + & - \\
- & + & - & - & - & + & + & - & + & - & 0 & + & + & - & - & + \\
- & - & + & - & - & - & + & + & + & + & - & 0 & + & + & - & - \\
- & + & + & + & - & - & - & - & + & - & - & - & 0 & + & + & + \\
- & - & - & + & + & - & + & - & + & + & + & - & - & 0 & - & + \\
- & + & - & - & + & - & - & + & + & - & + & + & - & + & 0 & - \\
- & - & + & - & + & + & - & - & + & + & - & + & - & - & + & 0
\end{array}\right)$$

where, for convenience, we have denoted 1 and -1 by $+$ and $-$ respectively. The ideal class group of $\mathbf{Z}[\frac{1}{2}(1+\sqrt{-15})]$ has order 2. The ideal $\mathcal{I} = \left\langle 2, \frac{1}{2}(1-\sqrt{-15}) \right\rangle$ is not principal and $\mathcal{I}L^+$ is given by construction A

from the binary code with the generator matrix

$$\begin{pmatrix}
1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0
\end{pmatrix}.$$

Thus $L_+[\mathcal{I}]$ is isometric to the orthogonal direct sum of two copies of the D_8^+ lattice. This is not isometric to L_+.

Another conference matrix of order 16 is

$$W_2 = \begin{pmatrix}
0 & + & + & + & + & + & + & + & + & + & + & + & + & + & + & + \\
- & 0 & + & + & - & + & - & - & + & - & + & + & - & + & - & - \\
- & - & 0 & + & + & - & + & - & + & - & - & + & + & - & + & - \\
- & - & - & 0 & + & + & - & + & + & - & - & - & + & + & - & + \\
- & + & - & - & 0 & + & + & - & + & + & - & - & - & + & + & - \\
- & - & + & - & - & 0 & + & + & + & - & + & - & - & - & + & + \\
- & + & - & + & - & - & 0 & + & + & + & - & + & - & - & - & + \\
- & + & + & - & + & - & - & 0 & + & + & + & - & + & - & - & - \\
- & - & - & - & - & - & - & - & 0 & + & + & + & + & + & + & + \\
- & + & + & + & - & + & - & - & - & 0 & - & - & + & - & + & + \\
- & - & + & + & + & - & + & - & - & + & 0 & - & - & + & - & + \\
- & - & - & + & + & + & - & + & - & + & + & 0 & - & - & + & - \\
- & + & - & - & + & + & + & - & - & - & + & + & 0 & - & - & + \\
- & - & + & - & - & + & + & + & - & + & - & + & + & 0 & - & - \\
- & + & - & + & - & - & + & + & - & - & + & - & + & + & 0 & - \\
- & + & + & - & + & - & - & + & - & - & - & + & - & + & + & 0
\end{pmatrix}.$$

In this case the lattice $\mathcal{I}L_+$ is obtained using construction A applied to the binary code with generator matrix

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0
\end{pmatrix}.$$

Thus $L_+[\mathcal{I}]$ is isometric to the D_{16}^+ lattice and so to L_+. This example shows that the isometry class of $L_+[\mathcal{I}]$ depends on the choice of the conference matrix W, and also that $L_+[\mathcal{I}]$ and $L_+[\mathcal{J}]$ may be isometric even when $\mathcal{I}$ and $\mathcal{J}$ are in different ideal classes.

References

[1] A. Bonnecaze, P. Solé & A. R. Calderbank, 'Quaternary quadratic residue codes and unimodular lattices' *IEEE Trans. Inform. Theory* **41** (1995), 366–377.

[2] R. Chapman & P. Solé, 'Universal codes and unimodular lattices', *J. Théor. Nombres Bordeaux* **8** (1996), 369–376.

[3] H. Cohn, *A Second Course in Number Theory*, John Wiley & Sons, 1962.

[4] P. M. Cohn, *Algebra* vol. 2 (2nd ed.), John Wiley & Sons, 1989.

[5] J. H. Conway & N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Springer-Verlag, 1988.

[6] J. Leech, 'Notes on sphere packing', *Canad. J. Math.* **19** (1967) 251–267.

[7] J .H. van Lint & R. M. Wilson, *A Course in Combinatorics*, Cambridge University Press, 1992.

[8] R. E. A. C. Paley, 'On orthogonal matrices', *J. Math. Phys.* **12** (1933), 311–320.

[9] J.-P. Serre, *A Course in Arithmetic*, Springer-Verlag, 1973.